

REMARKS

By this amendment, claims 1-14 are pending, in which no claims are canceled, currently amended, or newly presented.

The Office Action mailed March 1, 2007 rejected claims 1-14 under the judicially created doctrine of obviousness-type double patenting over claims 11-23 of U.S. Patent No. 6,778,498 B2.

Regarding the obviousness-type double patenting rejection, Applicant respectfully traverses on the merits because pending claims 1-14 are patentably distinct from those claims presented within commonly owned U.S. Patent No. 6,778,498 B2 (hereinafter ‘498 patent). The Examiner acknowledges that claims 11-23 of the ‘498 patent “do not explicitly contain ‘egress and ingress boundary router,’” but concludes that a best effort network somehow “incorporate the ingress and egress boundary routers in the best [sic] network of claims 11-23.” Applicants note that it is the use of the egress router vis-à-vis the ingress router is what enables protection from “denial of service attacks.” Nevertheless, even assuming, *arguendo*, that the Examiner’s assertion and resultant conclusion were proper, this does not justify ignoring the other claim language.

Specifically, the claims of the present application recite features not required by the claims of the ‘498 patent. As an example, the succeeding table highlights some patentably distinct differences between claim 1 (along with exemplary dependent claims 3-14) and claims 11-21 of the ‘498 patent.

Present Application 10/667,278	U.S. Patent 6,778,498 B2
---	---

<p>1. A network system, comprising: a network infrastructure providing a virtual private network (VPN) and a best effort public network; a first egress boundary router of said VPN and a second egress boundary router of said best effort public network that are each coupled for communication with an egress access network having an access link to which a destination host belonging to the VPN is coupled; a first ingress boundary router of the VPN and a second ingress boundary router of the best effort public network, wherein said first ingress boundary router transmits only packets originating from sources within the VPN and targeting the destination host to said first egress boundary router via said VPN, and wherein said second ingress boundary router transmits packets originating from sources outside the VPN and targeting the destination host to said second egress boundary router via said best effort public network; wherein at least said first egress boundary router is configured to transmit packets received via said VPN and targeting said destination host onto the egress access network utilizing a separate logical connection than that employed for packets communicated over the best effort public network, such that the access link is protected from denial of service attacks originating from sources outside the VPN.</p> <p>3. The network system of Claim 1, and further comprising: the egress access network connected to at least said first egress boundary router; and an ingress access network connected to at least the first ingress boundary router.</p> <p>4. The network system of Claim 3, wherein: said ingress access network is connected to each of said first ingress boundary router and said second ingress boundary router; said ingress access network has separate logical connections to said first and second ingress boundary routers for a customer premises equipment (CPE) edge router; and said ingress access network transmits</p>	<p>11. A network access system for use with an Internet protocol (IP) network infrastructure that implements a network-based Virtual Private Network (VPN) and a best effort network, said network access system comprising: a VPN-aware customer premises equipment (CPE) edge router, an access network supporting at least a first logical connection between the CPE edge router and network-based VPN and a second logical connection between the CPE edge router and the best effort network; wherein said VPN-aware CPE edge router includes: at least one customer network port having a connection for a customer network belonging to the VPN; at least one physical port on which at least first and second logical ports reside, said physical port having a physical port scheduler that transmits outgoing packets from said first logical port via said first logical connection and transmits outgoing packets from said second logical port via said second logical connection, wherein said physical port scheduler ensures access to said physical access link by outgoing traffic from said first logical port by one of (1) access link capacity allocation between outgoing traffic from said first and second logical ports and (2) access link prioritization of outgoing traffic from said first logical port over outgoing traffic from said second logical port; and a forwarding function configured to forward to said first logical port only packets identified as intra-VPN traffic to be communicated to a destination host belonging to the VPN and to forward other packets to said second logical port.</p> <p>12. The network access system of claim 11, wherein: said customer network port further includes a plurality of markers that each mark packets with a respective one of a plurality of service markings that each specify a different one of a plurality of qualities of service; at least said first logical port includes a plurality of queues each associated with a respective one of said plurality of qualities of service and a logical port scheduler that schedules transmission of packets from said plurality of queues; and said forwarding function places packets in particular ones of said plurality of queues in accordance with marking of said packets by said plurality of markers.</p> <p>13. The network access system of claim 12,</p>
--	---

packets having both source and destination addresses belonging to the VPN to said first ingress boundary router and transmits other packets to said second ingress boundary router.

5. The network system of Claim 4, and further comprising a CPE edge router coupled to said ingress access network, wherein said CPE edge router includes **a classifier that classifies at least some packets for routing to one of said first and second ingress boundary routers based at least in part on a host service markings in packet headers.**

6. The network system of Claim 3, wherein:
said egress access network is connected to each of said first egress boundary router and said second egress boundary router;
said egress access network has separate logical connections to said first and second egress boundary routers for a customer premises equipment (CPE) edge router; and
said first egress boundary router transmits packets from the VPN to said CPE edge router via a first of said logical connections and said second egress boundary router transmits packets from the best effort public network to said second ingress boundary router via a second of said logical connections.

7. The network system of Claim 6, wherein **said egress access network assigns a higher priority** to traffic received from said first egress boundary router than traffic received from said second egress boundary router.

8. The network system of Claim 7, wherein **said first egress boundary router shapes traffic** destined for the destination host to prevent starvation of traffic of said second egress boundary router that is destined for the destination host.

9. The network system of Claim 6, wherein **said first egress boundary router shapes traffic** destined for the destination host to a first rate and said second egress boundary router shapes traffic destined the destination host to a second rate, **wherein the sum of the first and second rates is no greater than a transmission capacity of said access link.**

10. The network system of Claim 1, wherein said first ingress router includes:
first and second logical input interfaces for receiving traffic destined for the VPN and for the best effort public network, respectively;

wherein each of said **plurality of markers marks packets** by setting a **Differentiated Services Code Point (DSCP)** in an Internet Protocol header of each marked packet.

14. The network access system of claim 11, wherein: **said customer network port includes a plurality of queues** each associated with a respective one of said plurality of qualities of service for outgoing packets destined for said customer network and a **customer network port scheduler** that **schedules transmission of packets from said plurality of queues**; and said forwarding function places packets received at said plurality of logical ports in particular ones of said plurality of queues in accordance with marking of said packets.

15. The network access system of claim 11, wherein said customer network port includes a **classifier that classifies at least some packets** as intra-VPN traffic based at least partially upon a source address and a partial destination address.

16. The network access system of claim 15, wherein **said classifier classifies** at least some packets **based at least partially upon a marking by a transmitter host.**

17. The network access system of claim 15, **said at least one customer network port** further **including at least one policer**, wherein **said classifier sends packets** to said **at least one policer for policing** in accordance with classification of said packets.

18. The network access system of claim 15, said classifier having an associated **classification table** that **associates particular values of packet header fields** with particular ones of said first and second logical ports.

19. The network access system of claim 11, wherein said **physical port scheduler allocates a first portion of access link capacity** to outgoing traffic from said first logical port and a second portion of access link capacity to outgoing traffic from said second logical port.

20. The network access system of claim 11, wherein said **physical port scheduler grants outgoing traffic** from said first logical port a higher access link priority than outgoing traffic from said second logical port.

first and second logical output interfaces for transmitting traffic over the VPN and the best effort public network, respectively; and

a forwarding function that switches packets received at said first logical input interface to said first logical output interface and that switches packets received at said second logical input interface to said second logical output interface.

11. The network system of Claim 10, wherein said first egress router includes:

first and second logical input interfaces for receiving traffic from the VPN and from the best effort public network, respectively;

a first logical output interface and a second logical output interface respectively coupled to separate first and second logical connections on said egress access network, wherein said first logical output interface transmits traffic received from the VPN utilizing said first logical connection and said second logical output interface transmits traffic received from the best effort public network utilizing the second logical connection; and

a forwarding function that switches packets received at said first logical input interface to said first logical output interface and that switches packets received at said second logical input interface to said second logical output interface.

12. The network system of Claim 11, wherein said first egress boundary router includes **a scheduler**, coupled to each of said first and second logical output interfaces, **that transmits packets from said first and second logical output interfaces onto said egress access network**, wherein said **scheduler grants a higher priority to traffic from said first logical output interface than to traffic from said second logical output interface**.

13. The network system of Claim 12, wherein said **scheduler performs work-conserving scheduling on outgoing traffic from said first and second logical output interfaces**.

14. The network system of Claim 11, wherein the VPN is one of a plurality of VPNs, and wherein said **forwarding function** has a corresponding plurality of **VPN forwarding tables and a shared forwarding table for best effort traffic**.

21. The network access system of claim 11, wherein said access network comprises **an L2 access network implemented with one of Asynchronous Transfer Mode, Ethernet and Frame Relay**.

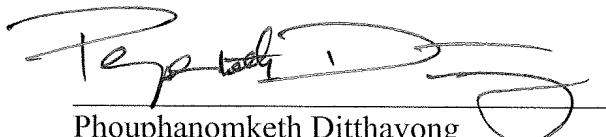
As evident from the claim chart, independent claim 1 of the present application recites features not required by claim 1 of the '498 patent. Claim 1 of the present application recites "wherein at least **said first egress boundary router is configured to transmit packets received via said VPN and targeting said destination host onto the egress access network** utilizing a separate logical connection than that employed for packets communicated over the best effort public network, such that **the access link is protected from denial of service attacks** originating from sources outside the VPN." Moreover, claim 11 of the '498 patent recites features not required by claim 1 of the present application, including "**a VPN-aware customer premises equipment (CPE) edge router.**" For at least these reasons, the claims of the present application are patentability distinct over claims 11-23 of the '498 patent.

Therefore, the present application, as amended, overcomes the rejection of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 519-9952 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

5/23/07
Date


Phouphanomketh Ditthavong
Attorney/Agent for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. (703) 519-9952
Fax. (703) 519-9958